International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 4, Issue 2, Apr 2014, 125-132

SYBIL ATTACK PREVENTION IN WIRELESS SENSOR NETWORK

MANJU V C

Research Scholar, Kerala University, Research Centre LBS Center, Kerala, India

ABSTRACT

Securing network protection in Wireless Sensor Networks (WSNs) increasingly becomes critical. There are many attacks that have been recognized in WSN till now by the researchers. Sybil attack is one of the harmful attacks against sensor network where a number of legitimate identities and forged identities are used to get an illegitimate entry into the network. Basically a Sybil attack means a node which pretends its identity like other nodes. In this scenario a node can trust the pretend node and it start sharing its information. Due to this activity a node's security is affected and information is lost. In this paper, a survey is done on Sybil attack and proposed a combined CAM – Compare and Match Approach and PVM Position Verification method to prevent these attacks.

KEYWORDS: Wireless Sensor Network, Sybil Attack, CAM, PVM

INTRODUCTION

Wireless sensor networks (WSN) have become a hot area of research due to the efficient design and implementation of sensor nodes. They are becoming less valuable and more powerful, enabling the promise of widespread use for everything from health monitoring to military application. Since wireless sensor networks are quite useful in many applications its security is highly important. Wireless networks are more vulnerable to malicious attacks, while wired and infrastructure based wireless networks have mature intrusion detection systems and sophisticated firewalls to block these attacks. Several types of attacks such as wormhole attack, sinkhole attack, selective forward attack, Sybil attack can be present in a network

A particularly harmful security attack against sensor networks is known as Sybil attack. Sybil attack is named after the subject of the book "Sybil", a case study of a woman diagnosed with multiple personality disorder. The name was suggested by Brian Zill at Microsoft research lab. However the Sybil attack had been used as an attacking service which deals with the reputation system for the peer to peer networks but as a result a large number of the entities had been created which are known as the pseudonymous. The Sybil attack had been the one which also takes into account the identities which had been generated from some cheaper results and apart from this some certain level of inputs also needs to be used when some of the entries had to be made into the entity. The entity is the term which is associated with the peer to peer networking but at times it may be worked with the help of the software so that the user may have some access to the resources. Sometimes both the identities and the entities needs to be mapped so that the proper results could be achieved by the user and even the faulty node may also be used when the user had to deal with the different forms of the identities.

In the latest network environment alien nodes can disguise in various identities and act as original nodes. Basically in social networks and defence networks there is no common master node for monitoring the peer to peer communication between network nodes .The analysis of peer to peer network shows that these networks are logical or *virtual* networks on top of already existing networks, i.e., they are mostly built upon below the network like the Internet.

Mostly P2P networks use their own addressing scheme' based on logical identifiers for structuring and forming the network.

SYBIL ATTACK AND ITS CLASSIFICATION

In sensor network hundreds of sensor nodes form the communication network. The wireless communication between these sensor nodes passes through a central station and these nodes communicate with fixed number of nodes. There are many encryption techniques available to prevent external attack of the nodes but nodes inside the communication network can also mount an attack. One of these insider attacks is called Sybil attack. Sybil attack is a type of spoofing attack where the attacker spoofs the identity of the normal node in the network and hence the messages directed to that victimized node are received by the attacker node.

Sybil attack would affect the geographical routing protocols and it can also reduce the effect of topology maintenance, fault tolerant schemes and distributed storage. Sybil attack is *explained* with the help of figure 1. In Sybil attack the node that spoofs the other node is called Sybil attacker or malicious node and the node whose identity get spoofed is called Sybil node. Here N is the normal node and S is a Sybil node. In proper communication only N nodes should communicate to each other. But here S node disguise itself as an internal known node and launches attack on the network. Sybil node tries to communicate with their neighboring node by using the identity of the normal node so a single node illegally presents multiple identities to other node in the network. Sybil node can be formed as a new identity or stealing legal identity So Sybil node is a misbehaving node's additional entity. This confuses the network and the network collapses.

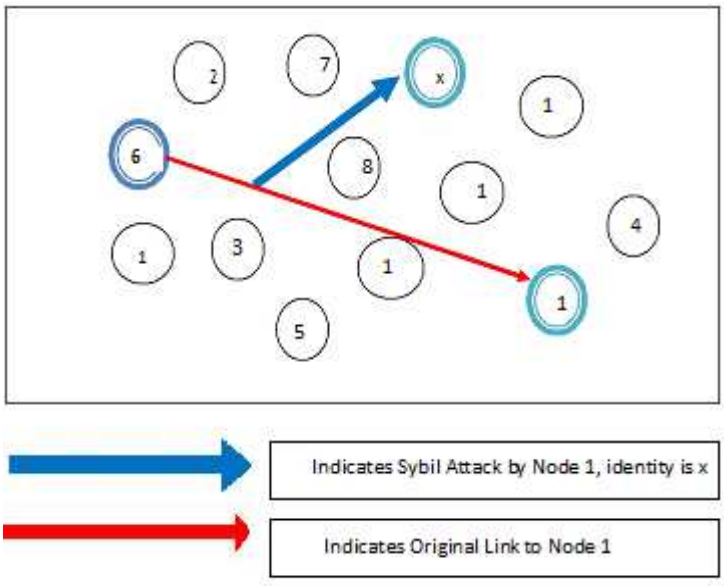


Figure 1: Sybil Attack

Sybil attacks are classified into three forms on the basis of how the network is attacked. They are

- **Direct Attack and Indirect Attack**

In direct attack, the original nodes communicate directly with Sybil nodes whereas in indirect attack the communication is done through malicious node.

- **Fabricated Attack and Stolen Identity Attack**

Legal identities of nodes are used to create new illegal node. I.e. if a sensor node has an ID of 16 bit integer then it creates the same ID of 16 bit, they are called fabricated nodes.

In stolen identities attacker identifies legal nodes and then uses it for malicious attack. The attack may go unidentified if the node whose identity has been stolen is destroyed. Identity replication is when the same identities are used many times in the same places.

- **Simultaneous and Non-Simultaneous Attack**

In simultaneous, all the Sybil identities participate in the network at the same time. Since only one identity appears at a time, practically cycling through identities will make it appear simultaneous. The number of identities the attacker uses is equal to the number of physical devices so each device presents different identities at different times. It is not simultaneous.

In Sybil attack, a malicious node can generate and control a large number of identities on a single physical device. This gives the illusion to the network as if it were different legitimate nodes. It can affect the following important protocol.

Distributed Storage

The same attack affects the architecture where it replicates the data on several nodes. Data will be stored on Sybil identities.

Routing

The nodes should be disconnected, but because of Sybil identities one node will be present in the different paths and locations.

Data Aggregation

One complete chunk of message is stored in a node. Due to the multiple identities of the Sybil nodes overall message would change. This would give wrong information.

Voting

In WSN most of the decisions are made by voting. Since the Sybil node has many identities a single node has a chance of voting many times, thus destructing the process.

Misbehavior Detection

A Sybil node acts as a legitimate node and this increases the trust of node. This increases the accuracy of a malicious node.

Fair Resource Allocation

Due to multiple identities of Sybil nodes it affects the resource allocation.

Defending Sybil Attack

Practically Sybil attack prevention is not that simple. One of the ways of preventing the attack is by having a central authority, such as an administrator who acts as a certifying authority. Administrator can guarantee that each person

has a single identity represented by one key. But in practice, this is very difficult to ensure on a large scale and would require costly manual attention.

Many algorithms on detecting and defending sybil attack other than having a central authority have been proposed. In this paper a new method called CAM is been proposed and combined with PVM is implemented. This approach is expected to give better performance for controlling the Sybil attack.

CAM

In this paper we are applying the CAM and PVM procedure to identify the Sybil node. If one approach fails to detect the attack then the other can catch like try catch method there are n number of nodes in the network.. Each node gets its own key value dynamically from the base station. Each node is connected by edge e. when nodes are starts communicating and sharing the data, each node should provide their key given by the base station. If the key is not matched with the key given by the base station, we can conclude that nodes are Sybil nodes. This is called CAM method,. The pseudo code of this CAM is given below.

In PVM, the detection of the Sybil node is done by verifying the position of the nodes. Whenever the nodes want to communicate with the other nodes, it should provide its original location. Basically the Sybil node always goes with the multiple identities. Here we are finding the Sybil node by identity wise as well as location wise. The performance of this paper is tested and verified using CAM-PVM method and it the simulation is done by NS2 code..

Compare and Matching (CAM)

- Create a group of n nodes.
- These n nodes connected by a link and each nodes are movable.
- One of the node is taken as the head node.
- K ={k_1,k_2,k_3……k_i k_j,…k_n} are the secret keys given by Head node to every nodes in the network. and K_i ← source node secret key Є K

  K_j ← destination node secret key Є K
- If (($key(v_i)$ == k_i) and ($key(v_j)$)== k_j)) then Vi send data to vj
- Then the Error msg comes as " Sybil node"
- End if
- End procedure

PVM [Position Verification Method]

- Create a group of n nodes.
- N nodes are connected by a link and the nodes are movable.
- X = {x_1,x_2,x_3……x_n} and Y={y_1,y_2,y_3,……y_n} andx_i, y_i values represents position of node n_i
- Node v_i, want to send data to node v_j

- $P_i \leftarrow$ source nodes position Є X,Y
- $P_j \leftarrow$ destination nodes position Є X,Y
- If ((vi(xi,yi) == Pi) and (vj (xj,yj)== Pj))then
- Vi sends data to vj
- Else the error msg shows“ Sybil node”
- End if
- End procedure

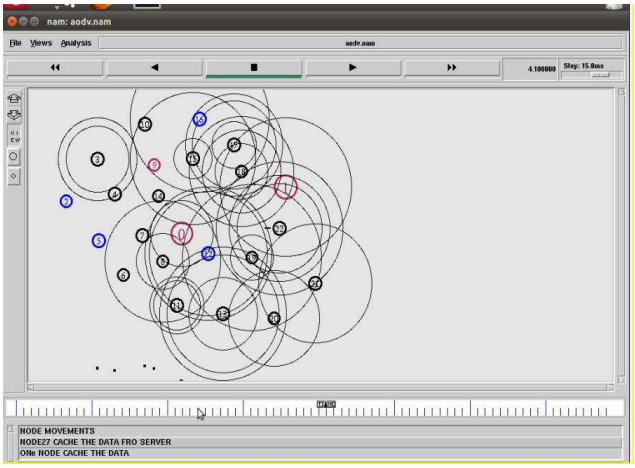


Figure 2

The simulation is done in NS2**,** with some 25 nodes connected in the network. Where all the nodes are moving node. They can have communication with each other and with their head node also. In this scenario, the node 5 is pretending its identity as 16 and start communicating to the severs. Now the node 5 is treated as Sybil node and whatever it communicate to the other node is called as Sybil attack. Sybil attack is shown by simulation in figure 2 and after applying the CAM PVM method the sybil node is identified in figure 3

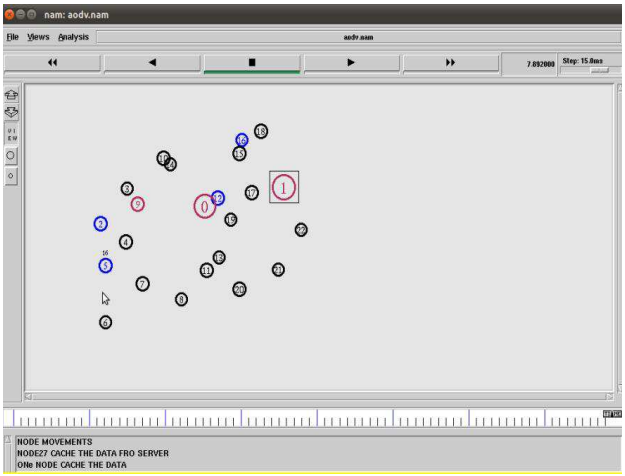
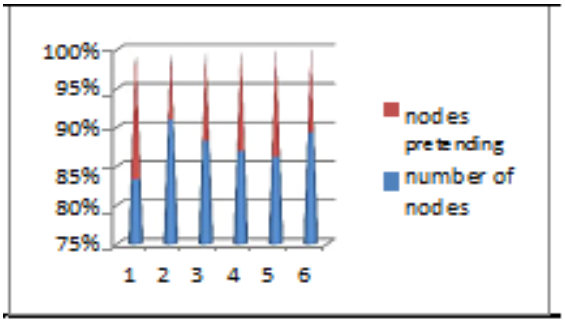


Figure 3

The ratio of the Sybil node in a WSN is analyzed and given in the following table.

Table 1: 12% of Sybil Nodes Appears in a WSN

Number of Nodes	Nodeo[S] Pretending
5	1
10	1
15	2
20	3
25	4
50	6



CONCLUSIONS

There are a variety of attacks that turning point on the issue of identity. In this paper, an analysis is done on Sybil attack and presented an overview of work related to defend the Sybil attack. We have demonstrated the breadth of applications that are subject to the attack, including the widely used systems Sensor network, social network, and others. The attack also presents a problem for peer-to-peer networks, mobile networks, and reputation systems. While we lack an efficient, general solution that scales well to large systems, there are a variety of solutions that can limit or prevent the attack in several individual application domains. Mainly our approach can solve the Sybil attack up to 88% in the WSN, hence proved.

REFERENCES

1. A survey of solutions to the Sybil attack. Brian Neil Levine Clay Shields, N. Boris Margolin.
2. N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In Proceedings of the ACM Workshop on Wireless Security (WiSe. 2003), September 2003.
3. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy, May 2003.
4. The Sybil Attack in Sensor Networks: Analysis & Defenses James Newsome Carnegie Mellon University.
5. A Survey of Solutions to the Sybil Attack, Brian Neil Levine R. Morselli, J. Katz, and B. Bhattacharjee.
6. A game-theoretic framework for analyzing trust-inference protocols. In 2nd Workshop on Economics of Peer-to-Peer Systems, Cambridge, MA, USA, June 2004.
7. M. Narasimha, G. Tsudik, and J. H. Yi. On the utility of distributed cryptography in p2p and manets: the case of membership control. In Proc. IEEE Intl Conference on Network Protocols (ICNP), 2003.

8. A. Acquisti, R.Dingledine, and P. Syverson. On the Economics of Anonymity. In Proc. Financial Cryptography (FC). Springer-Verlag, LNCS 2742, January 2003.
9. A. Adya, W. J. Bolosky, M. Castro, R. Chaiken, G. Cermak, J. R. Douceur, J. Howell, J. Lorch, M. Theimer, and R. P. Wattenhofer. Farsite: Federated, available, and reliable storage for an incompletely trusted environment. In Proc. OSDI, pages 1–14, Dec. 2002.
10. K. Anagnostakis and M. Greenwald. Exchange-based incentive mechanisms for peer-to-peer file sharing. In Proc. Intl Conference on Distributed Computing Systems (ICDCS), Mar. 2004.
11. J. Aspnes, C. Jackson, and A. Krishnamurthy. Exposing computationally challenged Byzantine impostors. Technical Report YALEU/DCS/TR-1332, Yale University Department of Computer Science, July 2005.
12. An RSSI based scheme for Sybil attack and detection in wireless sensor networks. Murat Demirbas, Youngwhan Song. Department of computer science and Engineering department. State university of New York at Buffalo.
13. Sybil Guard: Defending Against Sybil Attacks via Social Networks, Haifeng Yu Michael Kaminsky Phillip B. Gibbons Abraham Flaxman. Intel Research Pittsburgh Carnegie Mellon University
14. Detection of Sybil attack in mobile wireless sensor networks.S.Sharmila1, G Umamaheswari2